Houston Food Bank Client Data Collection, Sharing, Usage and Privacy Policy Outline: March 2020

Introduction The Houston Food Bank provides many services to hungry and vulnerable populations across the Gulf Coast region (our "clients"). These services include direct assistance through food distribution programs, as well as help with enrolling in State and Federal government benefit programs. We also work with a network of partners to help our clients get the help they need.

During the course of providing those services, we collect personally identifiable information, such as a client's name and address. This policy provides information about the rules in place for how we store, use, share, and protect the personal data of our clients.

We define personal data as any information that enables us to identify clients, directly or indirectly, by reference to an identifier such as name, identification number, location data, online identifier or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

The Houston Food Bank has core values regarding privacy. We aim to be transparent about the data we collect, how its used, and how users can opt-out. In general, we do not share personal data with law enforcement, with few exceptions (see below, "Why we collect personal data from clients").

Questions regarding this privacy policy should be directed to The Houston Food Bank by emailing HFBDataTeam@houstonfoodbank.org. Please reference this privacy policy in your subject line.

Who we are The Houston Food Bank provides food and resources across 18 counties in south east Texas. We are a registered 501(c)3 and part of Feeding America, the network of food banks across the United States.

Our Data Protection Officer can be contacted by sending an email to HFBDataTeam@houstonfoodbank.org or by mail to 535 Portwall St, Houston, TX, 77029.

What is personal data? The term "personal data" has different meanings in different jurisdictions. The State of Texas defines a few categories of personal data in Texas Business and Commerce Code Sec. 521.002:

- **Personal identifying information** is information “alone or in conjunction with other information” identifies an individual, including name, social security number, date of birth, government issued ID number, mother’s maiden name, unique biometric data, unique electronic ID number, and telecommunication access devices.
- **Sensitive personal information** is an individual’s first name or first initial and last name in combination with any of the following that is unencrypted: social security number, driver’s license or government ID number, account number or credit/debit card number in combination with a security code or password. Sensitive personal information can also include information that identifies an individual and relates to: physical or mental health condition, provision of health care, or payment for the provision of health care.

In this policy, we refer to both “personal identifying information” and “sensitive personal information” as “personal data” although the extent of data collection may not include all the fields defined in Texas law.

How we collect personal data from clients ***Personal data we collect from clients***
When clients participate in Houston Food Bank program, participate in an affiliated program, or visit a food pantry, they are asked to **optionally** provide their name, address, phone number, email address and other personal data such as housing type, language spoken, education level, employment type, monthly income, government assistance received, dietary considerations, demographic, and household information. The Houston Food Bank does not inquire about citizenship status. In some cases, this information is provided to us by partner organizations when clients sign up to participate in a Houston Food Bank-affiliated program.

Clients are also asked to disclose personal information, including income, when they apply for government benefits (e.g., SNAP) through Houston Food Bank’s Client Assistance Program. These data are stored and destroyed according to Texas Health and Human Services Commission rules and regulations.

Many HFB programs also ask clients to answer surveys about topics such as their level of food insecurity, as well as their feedback and experiences. In these survey responses, clients may choose to offer personal data as part of their free form text response.

Personal data collected from food pantries Each time a client visits a food pantry and receives food, we log their visit and record information about the amount of food

received. This information is stored in their client profile.

Personal data we collect from partner organizations Houston Food Bank collects client data about their participation and outcomes in HFB-affiliated programs run by partner organizations, such as Food Scholarship and FoodRx. The type and detail of data shared with HFB varies depending on the program and the data sharing agreement signed by both parties, but can include attendance, completion of program, and outcomes measures of health, education, or economics. In all cases, clients are informed about the data that will be shared with HFB prior to enrolling and consent to the partner organization sharing their data with HFB.

Why we collect personal data from clients

We collect personal data from clients for the following reasons:

- *To Improve Our Programs*: We may use your information to improve our programs or activities. For example, our staff may look at information to review the quality of services that people receive.

- *To Do Research*: We may use your information for research and analysis. Any reports produced with the data will not identify your individual information. Our staff and volunteers will only share your information with qualified persons outside of our agency.

- *To Connect Clients with Other Programs*: At a client's request, we may share their personal information to see if they are eligible for other benefits or programs such as Social Security benefits or SNAP.

- Houston Food Bank **will not** disclose personal data unless court ordered or compelled by law. We are required by law to report any cases of suspected abuse or neglect of children or vulnerable adults. We are also required to share information about clients to law enforcement if they cause harm to a member of our staff, another client, or if they damage our property. We may also share personal information in case of a threat to the public, such as a natural disaster or potential danger to others.

When data is shared with third-parties The Houston Food Bank does not sell personal data or share it with unauthorized third-party vendors.

We may share data about food pantry participation with partner organizations for research purposes. We only share personal data with partner organizations who have signed a data sharing agreement and agree to keep personal data secure in accordance with our privacy and security policies.

How we store data and keep it secure *Client and pantry data stored in Link2Feed* In most cases, personal data about food pantry visits are recorded and stored through Link2Feed, the Houston Food Bank's food pantry and client management software technology.

- Link2Feed is bound by a detailed licensing and confidentiality agreement that affirms no ownership to your food bank's data or user information.

- At no point will Link2Feed release your data to the public or sell it to an affiliate.

- Link2Feed's 256-bit security encryption per field is the same level of online banking providers. The Link2Feed system automatically assesses all browser security settings prior to accessing the online system to ensure the highest level of data protection.

- Every authorized user is required to read, understand and sign (by logging in) an End User License Agreement (EULA). The system automatically sends an agreement through the Link2Feed software that all users must click to accept in order to login.

- All staff and volunteers must have their own login to Link2Feed. Usernames or passwords are not to be shared.

- User roles are assigned to every end user/intake person with varying levels of permissions to access client data. It is the responsibility of the Agency Manager to conduct regular maintenance of overview of users and roles.

- Client data is more secure in Link2Feed since pieces of paper on a desk or stored in unlocked file cabinets are vulnerable to copying.

For additional security information about Link2Feed:

http://Link2Feed.com/security-features/

HFB has no control over how information is received, stored, or used when data is collected using systems other than HFB provided systems, such as Link2Feed, at affiliated locations.

Community Assistance Programs Data Personal data collected through Houston Food Bank's client assistance programs that help clients apply for government benefits are stored separately from data stored on Link2Feed.

- When clients are applying for government assistance programs, such as SNAP, HFB staff records personal information required by law to qualify for benefits. HFB does not keep or store this data. It is encrypted and sent to the State Health and Human Services.

- HFB also records limited personal information about applicants in a separate datafile on a secure and encrypted laptop (VPN internet only). In compliance with HHSC rules and regulations, these personal data are encrypted and stored for 120 days on a secure server and then destroyed.

- HFB stores aggregate monthly counts of the number of applications completed with aggregate breakdowns by geographic area. No personal information is stored for these purposes.

Client Survey Data HFB occasionally provides follow up surveys to our clients. In those cases, HFB either (1) uses the internal survey modules from Link2Feed, which are subject to the same security requirements as the rest of the Link2Feed system, or (2) uses other software products that maintain compliance with major standards, such as HIPAA, PCI, and FERPA. Surveys may require personal information, but such is only provided by you voluntarily.

Client Data Collected By Partner Organizations HFB may collect data from external partners in order to track the outcomes of shared programs. These partner organizations provide data by uploading files to HFB's cloud storage. It is a fully encrypted cloud storage system.

Data Security Incidents A data security incident is an unauthorized acquisition of

data that compromises the security, confidentiality, or integrity of personal data. HFB takes data security very seriously, and employs the multiple security features to help reduce the likelihood of a data breach.

It is important to note that these procedures exist to guide HFB's internal teams and external vendors in the event of a data security incident.

In the event of a confirmed data security incident, HFB may be required by Texas law to follow certain procedures relating to the investigation, disclosure, and remediation of the data breach.

- Disclose the data security incident to any individuals who HFB believes to have had their personal data acquired by an unauthorized person.
- Notify any personnel who manage systems that store personal data.
- In certain cases, notify consumer reporting agencies.

HFB takes data security very seriously. In addition to the potential notification procedures, HFB also has the following internal audit procedures in the event of a confirmed data security incident:

- Immediately stop unauthorized access by identifying and closing methods of intrusion.
- Determine, to the best of our ability, why the data breach occurred, and what long-term technical and procedural patches need to occur.
- Remediate any damage caused by unnecessary access.

Data Encryption Data encryption is a security measure that can help prevent unauthorized access of personal data in the event of a network intrusion, a stolen device, or other common scenarios. It acts as a safeguard to help ensure that personal data cannot be seen by unauthorized personnel unless they are able to decrypt the data, which presents an additional, sophisticated hurdle.

- HFB uses data encryption in a variety of ways, including:
    - Device hard drive and boot disk encryption. All HFB-issued devices with access to sensitive data, such as laptops and desktops, use hard drive encryption.
    - External device encryption. It is HFB's policy not own, use, or manage mobile devices, SD cards, or thumb drives with access to sensitive

information.

○ Email encryption. Sensitive data transmitted by email is encrypted end-to-end.

○ File and folder encryption. Specific files used to track clients and client outcomes are encrypted and password protected.

○ Encryption in transit. Personal data sent from one device to another over a network is encrypted end-to-end.

Changes to this policy If we make any material changes to this Data Collection and Privacy Policy or the way we use, share or collect personal data, we will notify you by revising the “Effective Date” at the top of this Policy and prominently posting an announcement of the changes on our website prior to the new policy taking effect.

Any changes we make to our Data Collection and Privacy Policy in the future will be posted on this page and, where appropriate, notification sent to you by email. Please check back frequently to see any updates or changes to this Policy.